METHOD AND APPARATUS FOR DATA NORMALIZATION

Abstract of Disclosure

A method that allows the normalization of traffic data that is simultaneously transferred to a network intrusion detection system (NIDS) and monitored end-systems located in a network, such as a TCP/IP network, in which packets of data such as IP datagrams, are fragmented and reassembled. Accordingly, the information of received fragments and/or the topology of the network comprising the network intrusion detection system (NIDS) and the monitored end-systems are entered into a normalization table, that is dynamically established and maintained. Subsequently packets of data such as IP datagrams are modified, redirected or discarded in case that ambiguities are detected when comparing information contained in the normalization table with information contained in the headers of the received data packets.

Figures